IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

KIM WHITE, an individual, on behalf of herself and all others similarly situated, Plaintiff, v. CGM LLC, d/b/a CGM, Inc., Defendant.	Civil Action No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, on behalf of herself and all persons similarly situated, alleges:

NATURE OF THE CASE

1. This is a consumer class action lawsuit brought by Plaintiff, individually and on behalf of all others similarly situated (i.e., the Class Members), who entrusted Defendant CGM LLC d/b/a CGM, Inc. ("CGM" or "Defendant") to safeguard their personally identifiable information ("PII"), which includes without limitation name, driver's license numbers, and/or state identification card numbers.

2. CGM has failed to comply with industry standards to protect information in its systems that contain PII, and has failed to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII had been compromised. Plaintiff seeks, among other things, orders requiring CGM to fully and accurately disclose the nature of the information

that has been compromised and to adopt reasonably sufficient security practices and safeguards to prevent incidents like this in the future.

3. CGM experienced a data security incident between December 15, 2022 and December 28, 2022 that involved Plaintiff's and other consumers' PII (the "Data Breach"). As a result, an unauthorized party accessed certain files within the Defendant's systems and may have viewed, acquired, and/or exfiltrated data containing affected parties' PII. The security incident was wide-reaching, effecting a number of the Defendant's computer systems and compromising the PII of more than 279,000 people.

4. As a result of Defendant's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of criminals. Plaintiff and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to the Defendant's failures.

5. Accordingly, Plaintiff, individually and on behalf of all others similarly situated, alleges claims for negligence and negligence *per se*, breach of implied contract, unjust enrichment, and injunctive/declaratory relief.

PARTIES

6. Plaintiff Kim White is domiciled in Springfield, Ohio and is a citizen of the State of Ohio. Plaintiff's PII was collected and maintained by CGM and disclosed without authorization to an unknown and unauthorized third party as a result of the Data Breach. *See* Exhibit 1 attached hereto for a copy of the Notice Letter that Plaintiff received regarding the Data Breach.

7. Defendant CGM is a software development and data processing company that provides services to help wireless and broadband companies participate in the federal Affordable Connectivity Program and Lifeline Program. Due to the nature of the services it provides, CGM regularly acquires and electronically stores PII belonging to consumers as part of the regular course of its business. CGM is a Georgia corporation with a principal place of business located at 104 Sloan Street, Roswell, Georgia, 30075.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

9. This Court has personal jurisdiction over Defendant because Defendant resides in this District, at all relevant times it has engaged in substantial business activities in Georgia.

10. Pursuant to 28 U.S.C. § 1391(b)(1) and (2), venue is proper in this District because this is where the Defendant resides and is where a substantial part of the events or omissions giving rise to the claims occurred.

BACKGROUND AND FACTS

11. In June of 2023, Defendant publicly disclosed that it had "observed unusual activity related to certain systems within [its] network."[1]

[1] *See* https://ago.vermont.gov/sites/ago/files/2023-06/2023-06-07%20CGM%20Data%20Breach%20Notice%20to%20Consumers.pdf (last visited June 16, 2023).

12. Defendant initiated an investigation and engaged cybersecurity experts to determine the size and scope of the breach. On December 28, 2022, CGM learned that between December 15, 2023 and December 28, 2023, there was a data security incident involving Plaintiff's and class members' PII.

13. Defendant and its cybersecurity experts then conducted an investigation that determined that in fact, consumers' PII, including the Plaintiff's PII, was put at risk. The security incident was wide-reaching, affecting a number of the organization's computer systems and compromising the PII of more than 279,0000 people.

14. Defendant mailed notification letters to all affected individuals informing them about the Data Breach. In these letters, Defendants offered affected individuals the opportunity to enroll in free credit monitoring and identity restoration services through a product sold by TransUnion.

15. The Notification Letters were deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, when Defendant completed its investigation, why sensitive information was stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the stolen data was encrypted or otherwise protected, and whether Defendant knows if the data has not been further disseminated.

16. In deliberate disregard of the fact that the stolen sensitive information was accessed by an unauthorized third party, CGM downplayed the seriousness of the incident by failing to take steps necessary to inform Plaintiff and Class Members that their data was in fact stolen by third party bad actors, and that CGM, seemingly more out of an abundance of caution, wanted to make Plaintiff and Class Members aware of the Data Breach.

17. CGM acknowledges that it is responsible to safeguard Plaintiff and Class Members' PII. It pledges that it takes privacy very seriously and makes numerous promises that it will maintain the security and privacy of PII.

18. Consumers who participated in government programs, such as Plaintiff, entrusted their PII to CGM with the mutual understanding that this highly sensitive private information was confidential and would be properly safeguarded from misuse and theft.

19. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, CGM assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class Members' PII from disclosure.

20. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and they rely on CGM to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

21. CGM was well aware that the PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes. As the Federal Trade Commission (FTC) recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and fraud.[2] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

[2] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited June 2, 2023).

22. The ramifications of Defendant's failure to keep PII secure are long lasting and severe. Once stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

23. Further, criminals often trade stolen PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

24. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[3] This time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

25. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

26. Further, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of

[3] *Identity Theft and Your Social Security Number*, Social Security Administrative, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed June 2, 2023).

misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

27. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[4]

28. Defendant knew, or should have known, the importance of safeguarding PII entrusted to it and of the foreseeable consequences if its systems were breached. This includes the significant costs that would be imposed on individuals as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

29. Plaintiff and Class Members now face years of constant surveillance of their records. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

30. Despite all of the publicly available knowledge of the continued compromises of PII, CGM's approach to maintaining the privacy of the PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

[4] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited June 2, 2023).

31. In all contexts, time has constantly been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be spared having to deal with the consequences of Defendant's misfeasance.

32. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

33. The delay in identifying and reporting the Data Breach caused additional harm to Plaintiff and Class Members. Plaintiff was not timely notified of the Data Breach, depriving her and the Class of the ability to promptly mitigate potential adverse resulting consequences.

34. As a result of CGM's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

a. Actual identity theft;

b. Unauthorized use and misuse of their PII;

c. The loss of the opportunity to control how their PII is used;

d. The diminution in value of their PII;

e. The compromise, publication, and/or theft of their PII;

f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

g. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

h. Costs associated with placing freezes on credit reports;

i. Delay in receipt of tax refund monies or lost opportunity and benefits of electronically filing of income tax returns;

j. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

k. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as it fails to undertake appropriate measures to protect the PII in its possession; and

l. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

35. To date, CGM has not yet disclosed full details of the Data Breach. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, it has taken to secure the PII still in its possession. Through this litigation, Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses any harms, and ensure CGM has proper measures in place to prevent another breach from occurring in the future.

36. CGM was expressly prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

37. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[5]

38. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[6] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

39. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

40. CGM failed to properly implement basic data security practices. Its failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

---

[5] Federal Trade Commission, *Start With Security: A Guide for Business*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed June 2, 2023).

[6] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed June 2, 2023).

41. CGM was at all times fully aware of its obligation to protect PII and was also aware of the significant repercussions that would result from its failure to do so.

CLASS ACTION ALLEGATIONS

42. Plaintiff brings this action on behalf of herself and all others similarly situated (the "Class'). Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All individuals whose PII was maintained by CGM and who were sent a notice of the 2023 Data Breach.**

Plaintiff Kim White also brings her claims on behalf of a Subclass of Ohio victims with subclass to be defined as follows:

> **All Ohio individuals whose PII was maintained by CGM and who were sent a notice of the 2023 Data Breach.**

43. Excluded from the Class are Defendant, Defendant's subsidiaries and affiliates, its officers, directors, and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representatives, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

44. Plaintiff reserves the right to modify or amend the definition of the proposed Class and Subclass and/or to add classes or subclasses, if necessary, before this Court determines whether certification is appropriate.

45. Numerosity: The Class Members are so numerous that joinder of all Members is impractical. The Class is comprised of over 279,000 individuals. Defendant has the

administrative capability through its computer systems and other records to identify all members of the Class and Subclass, and such specific information is not otherwise available to Plaintiff.

46. Commonality: The questions here are ones of common or general interest such that there is a well-defined community of interest among the Members of the Class and Subclass. These questions predominate over questions that may affect only individual class members because CGM has acted on grounds generally applicable to the Class and Subclass. Such common legal or factual questions include, but are not limited to:

a. Whether and to what extent Defendant had a duty to protect the PII of Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class Members' PII;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

i. Whether Plaintiff and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach; and

o. Whether Plaintiff and Class Members are entitled to additional identity theft protection.

47. Typicality: Plaintiff's claims are typical of the claims of the other members of the Class because Plaintiffs' PII, like that of every other Class Member, was not properly maintained or secured by Defendant. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of CGM. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

48. It is impracticable to bring the individual claims of the members of the Class and Subclass before the Court. Class treatment permits a large number of similarly situated persons or entities to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that numerous individual actions would engender. The benefits of the class mechanism, including providing injured persons or entities with a method for obtaining redress on claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action.

49. Adequacy of Representation: Plaintiff is a more than adequate representative of the Class in that Plaintiff's PII was compromised and has suffered damages. In addition:

a. Plaintiff is committed to the vigorous prosecution of this action on behalf of herself and all others similarly situated and has retained competent counsel experienced in the prosecution of class actions and, in particular, class actions regarding data breaches;

b. There is no conflict of interest between Plaintiff and the unnamed members of the Class or Subclass;

c. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and

d. Plaintiff's legal counsel have the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

50. Plaintiff knows of no difficulty to be encountered in the maintenance of this action that would preclude its maintenance as a class action.

51. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

52. CGM has acted or refused to act on grounds generally applicable to the Class and Subclass, thereby making appropriate corresponding declaratory relief with respect to the Class and Subclass as a whole. CGM's actions and inactions challenged herein apply to and affect Class Members uniformly and hinges on its conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

53. Superiority of Class Action. The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other

available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against a large organization like Defendant. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

54. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

55. The litigation of the claims brought herein is manageable. CGM's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

56. Adequate notice can be given to Class Members directly using information maintained in CGM's records.

57. Unless a Class-wide injunction is issued, CGM may continue in its failure to properly secure the PII of Class Members, may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and may continue to act unlawfully as set forth in this Complaint.

58. All conditions precedent to bringing this action have been satisfied and/or waived.

FIRST CAUSE OF ACTION
Negligence and Negligence *per se*
(On Behalf of Plaintiff and the Class)

59. Plaintiff and the Class re-allege and incorporate by reference each and every preceding paragraph of this Complaint.

60. Defendant had a duty to exercise reasonable care to protect and secure Plaintiff's and the Class Members' PII.

61. Through its acts and omissions, Defendant violated its duty to use reasonable care to protect and secure Plaintiff's and Class Members' PII as set forth herein and as follows:

a. Defendant failed to physically or electronically protect and secure Plaintiff's and Class Members' PII;

b. Defendant retained Plaintiff's and Class Members' PII longer than was reasonably necessary; and,

c. Defendant failed to disclose the security breach in the most expedient time possible and without unreasonable delay to Plaintiff and Class Members.

62. Defendant breached the duties owed to Plaintiff and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of information that resulted in the

unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow its own privacy policies and practices.

63. It was reasonably foreseeable that Defendant's failure to exercise reasonable care to protect and secure Plaintiff's and Class Members' PII would result in an unauthorized third-party gaining access to, possession of, and control over such information for an unlawful purpose.

64. Defendant's failure to adequately protect Plaintiff's and Class Members' PII was negligent.

65. Plaintiff's and Class Members' PII constitute personal property and due to Defendant's negligence their PII was exposed or stolen, resulting in harm to Plaintiff and Class Members.

66. Defendant's negligence directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII and Plaintiff and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described herein.

67. Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as

CGM or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of CGM's duty.

68. CGM violated Section 5 of the FTCA by failing to use reasonable measures to protect PII and not complying with the industry standards. CGM's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a Data Breach.

69. Plaintiff and Members of the Class are consumers within the class of persons Section 5 of the FTCA was intended to protect.

70. CGM's violation of Section 5 of the FTCA constitutes negligence *per se*.

71. The harm that has occurred as a result of its conduct is the type of harm that the FTC Act was intended to guard against.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

72. Plaintiff and the class re-allege and incorporate by reference each and every preceding paragraph of this Complaint.

73. When Plaintiff and members of the Class provided their personal information to CGM, Plaintiff and members of the Class entered into implied contracts with CGM pursuant to which CGM agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their data had been breached and compromised.

74. Defendant required Plaintiff and class members to provide and entrust their PII and financial information as a condition of obtaining Defendant's services.

75. Plaintiff and Class members would not have provided and entrusted their PII and financial information to CGM in the absence of the implied contract between them and CGM.

76. Plaintiff and members of the Class fully performed their obligations under the implied contracts with CGM.

77. CGM breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the personal information of Plaintiff and members of the Class and by failing to provide timely and accurate notice to them that their personal information was compromised in and as a result of the Data Breach.

78. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of CGM's breaches of the implied contracts between CGM and Plaintiff and members of the Class.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

79. Plaintiff and the Class restate and reallege all proceeding allegations above as if fully set forth herein.

80. This count is brought in the alternative to Plaintiff's breach of contract count. If claims for breach of contract are ultimately successful, this count will be dismissed.

81. Plaintiff and Class members conferred a benefit on CGM by way of customers' paying CGM to maintain Plaintiff and Class members' personal information.

82. The monies paid to CGM were supposed to be used by CGM, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class members.

83. CGM failed to provide reasonable security, safeguards, and protections to the personal information of Plaintiff and Class members, and as a result CGM was overpaid.

84. Under principles of equity and good conscience, CGM should not be permitted to retain the money because CGM failed to provide adequate safeguards and security measures to protect Plaintiff's and Class members' personal information that they paid for but did not receive.

85. CGM wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class members.

86. CGM's enrichment at the expense of Plaintiff and Class members is and was unjust.

87. As a result of CGM's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by CGM, plus attorneys' fees, costs, and interest thereon.

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

88. Plaintiff and the Class restate and reallege all proceeding allegations above as if fully set forth herein.

89. This cause of action is brought under 28 U.S.C. § 2201. This Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious as described in this Complaint.

90. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate, contrary to its assertion that it has confirmed the security of its network and its systems.

91. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of PII and remains at imminent risk that further compromises will occur in the future.

92. This Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure PII and to timely notify those affected of the Data Breach; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure PII.

93. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect PII.

94. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach. The risk of another such breach is real, immediate, and substantial. If another breach at CGM occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

95. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to CGM if an injunction is issued. Plaintiff will likely be subjected to substantial

identity theft and other damage. On the other hand, the cost to CGM of complying with an injunction by employing reasonable prospective data security measures and communicating those measures to the Class is relatively minimal, and it has a pre-existing legal obligation to employ such measures.

96. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at CGM, thus eliminating the additional injuries that would result to Plaintiff and to those whose PII would be further compromised.

97. Plaintiff and the Class, therefore, seek a declaration (1) that CGM's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their obligations and duties of care, CGM must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment PII data by, among other things, creating firewalls and access controls so that if one area of Defendant's system is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner all data not necessary for its provisions of services;

f. Ordering that Defendant conduct regular computer system scanning and security checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendant to meaningfully educate employees and members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all other similarly situated, prays for relief as follows:

A. For an order certifying the Class and Subclass and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and

H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Date: June 19, 2023

Respectfully submitted,

BY: WEBB, KLASE & LEMOND, LLC

/s/ G. Franklin Lemond, Jr.

E. Adam Webb
Georgia Bar No. 743910
G. Franklin Lemond, Jr.
Georgia Bar No. 141315

1900 The Exchange, S.E.
Suite 480
Atlanta, Georgia 30339
(770) 444-9325
(770) 217-9950 (fax)
Adam@WebbLLC.com
Franklin@WebbLLC.com

Kenneth J. Grunfeld*
Kevin W. Fay*
GOLOMB SPIRT GRUNFELD
1835 Market Street, Suite 2900
Philadelphia, PA 19103
Phone: 215-985-9177
kgrunfeld@golomblegal.com
kfay@golomblegal.com

Attorneys for Plaintiff and Proposed Class

**Pro hac vice or applications for admission to be filed*